Google Scholar BETA

Web Images Video News Maps more »

VMM TPM hypervisor Search

Advanced Scholar Search
Scholar Preferences
Scholar Help

Scholar **All articles** - Recent articles Results **1** - **10** of about **101** **English** pages for **VMM TPM hypervisor**. (**0.10** seconds)

An Approach to a Trustworthy System Architecture Using Virtualization - •tu-darmstadt.de [PDF]
F Stumpf, M Benz, M Hermanowski, C Eckert - LECTURE NOTES IN COMPUTER SCIENCE, 2007 - Springer
... I/O emulation is moved into the **hypervisor** layer ... The **VMM** establishes several different execution environments by using ... of the underlying hardware **TPM** through a ...
Cited by 6 - Related articles - Web Search - BL Direct - All 4 versions

[PDF] •vTPM: Virtualizing the Trusted Platform Module
R Perez, R Sailer, L van Doorn - usenix.org
... said to be par- avirtualized, otherwise the **VMM** is said ... A virtual **TPM** should provide **TPM** services to each vir- tual machine running on top of a **hypervisor**. ...
Cited by 32 - Related articles - View as HTML - Web Search - All 6 versions

12 IBM. IBM eServer x366. http://www-03. ibm. com/servers/eserver/xseries/x366. html. 13 IBM. ... - •usenix.org [PDF]
S Coprocessing, SH Standard, XOS Hypervisor - IEEE Computer, 2005 - usenix.org
... said to be par- avirtualized, otherwise the **VMM** is said ... A virtual **TPM** should provide **TPM** services to each vir- tual machine running on top of a **hypervisor**. ...
Related articles - View as HTML - Web Search - All 2 versions

[HTML] •Implementation for Xen
PHTPMPT VM - usenix.org
... virtual **TPM** support for the Xen **hypervisor** [27 ... the two previously discussed solutions of a virtual **TPM**. ... Xen is a **VMM** for paravirtualized operating systems that ...
Cached - Web Search

Building a MAC-Based Security Architecture for the Xen Open-Source **Hypervisor** - •ibm.com [PDF]
R Sailer, T Jaeger, E Valdez, R Caceres, R Perez, ... - ieeexplore.ieee.org
... and its integration into the Xen **VMM** system. ... VMs, isolation of virtual resources, and **TPM**-based attestation ... manage the security policies for the Xen **hypervisor**. ...
Cited by 60 - Related articles - Web Search - All 17 versions

Linking remote attestation to secure tunnel endpoints - •ibm.com [PDF]
K Goldman, R Perez, R Sailer - Proceedings of the first ACM workshop on Scalable trusted ..., 2006 - portal.acm.org
... physical platform and software through the **hypervisor** and **TPM** partition the ... connecting the AIK to the platform running the **hypervisor** the self ... **VMM**-**Hypervisor** ...
Cited by 13 - Related articles - Web Search - All 3 versions

Enabling platform network stack control in a virtualization platform
SL Grobman - US Patent App. 10/954,905, 2004 - Google Patents
... In a **hypervisor** model, multiple operat- ing systems may be run in VMs as peers on ... If a virus maliciously modifies the **VMM**, **TPM** will not allow the **VMM** to launch ...
Web Search

Trust Maintenance Toward Virtual Computing Environment in the Grid Service
D Wang, A Wang - LECTURE NOTES IN COMPUTER SCIENCE, 2008 - Springer
... Page 6. Trust Maintenance Toward Virtual Computing Environment in the Grid Service 171 **TPM Hypervisor VMM** Virtual Machine Monitor **TPM**-PROXY Meas. ...
Related articles - Web Search - BL Direct - All 2 versions

[PDF] •Enhancing Trusted Platform Modules with Hardware-Based Virtualization Techniques
F Stumpf, C Eckert - 2008 - sec.informatik.tu-darmstadt.de
... 16] and the other on the Xen **hypervisor** [9]. These ... vmentry and the transition back to the **VMM** is called ... But in contrast to directly integrating a **TPM** into the ...
View as HTML - Web Search

A **hypervisor**-based system for protecting software runtime memory and persistent storage
P Dewan, D Durham, H Khosravi, M Long, G ... - Proceedings of the 2008 Spring simulation multiconference, 2008 - portal.acm.org
... In virtualization systems, the **VMM** maintains a separate set of page ... known to the **hypervisor**) can be bootstrapped from **TPM** when the **hypervisor** is launched. ...
Web Search

Key authors: **R Sailer** - **R Perez** - **L van Doorn** - **S Berger** - **T Jaeger**

Gooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

VMM TPM hypervisor Search